HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/81C

12 January 2017

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority (HKMA) published today the seventh issue of the Operational Incidents Watch (see enclosure).

The Operational Incidents Watch is a periodic newsletter to share with the industry the major lessons learnt from selected significant operational incidents that have happened in the banking sector. It aims at facilitating authorized institutions (AIs) and members of the public to stay alert and to take appropriate measures to prevent similar incidents from happening to them. The HKMA expects the senior management of AIs to take steps to ensure that their business lines or operational risk management functions will take into account the incidents described in the Operational Incidents Watch in reviewing and enhancing where necessary their institutions' risk management controls.

If you have any questions about the Operational Incidents Watch, please contact Mr Parry Tang at 2878-1524 or Ms Christie Yee at 2878-1620.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl

Issue No. 7
12 January 2017

Operational Incidents Watch is a periodic newsletter published by the Banking Supervision Department of the Hong Kong Monetary Authority (HKMA). It summarises the major lessons learnt from selected operational incidents[1] that have happened in the banking industry and led to impact on customers or material financial losses to the authorized institutions (AIs) concerned. It aims at facilitating AIs and members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them.

In this newsletter, the modus operandi and the factors and key control loopholes leading to two operational incidents are outlined. These two incidents involved (i) insufficient evaluation of credit card applications; and (ii) incorrect trade capture of plain OTC derivatives transactions.

Insufficient evaluation of credit card applications

Fraudsters used fictitious identities to apply credit cards and the applications were accepted without adequate evaluation.

Modus operandi / factors leading to the incident

Fraudsters made use of copies of fake HKID cards and income proof and address proof documents of fictitious individuals to apply for credit cards from victim AIs (through the AIs' drop-in boxes or direct sales booths). As these applicants did not actually exist, the credit reports obtained from the credit reference agency by the AIs showed "nil" records. However, the credit officers of the AIs treated these applicants as first-time applicants of credit facilities who had no record with the credit reference agency (i.e. new-to-bureau applicants) without further evaluation. The applications were therefore approved and the credit cards were issued.

[1] Because of sensitivity, the incidents mentioned in this newsletter may be prepared on the basis of synthesis of multiple incidents and certain details of the incidents may deliberately be omitted.

As the fraudsters selected some old buildings with lax security of their mailboxes as the "addresses" of the fictitious applicants, they were able to pick up the letters sent by the AIs containing the credit cards and PINs and then activate the credit cards. Subsequently, the AIs identified unusual activities in these credit card accounts and reported the cases to the Police, which then arrested the fraudsters.

Control loopholes and lessons learnt

i. Some front-line staff members failed to follow the AIs' control procedures to obtain original identification documents of the applicants for verification when they received the applications at the direct sales booths. The responsible front-line staff members were reminded of these control procedures and these relevant procedures were also enhanced.

ii. Where a "nil" record is shown in a credit report obtained from the credit reference agency, the AIs' credit officers should have regarded it as a potential fraud risk factor for further evaluation or verification of the applications. In addition, the delivery of credit cards to this type of customers should also be handled with greater care, for example, through registered mails or requiring the collection of credit cards at branches.

iii. As the fraudsters tended to submit multiple credit card applications by making use of the same addresses and/or phone numbers, AIs may consider including this risk factor into their fraud detection systems/tools to facilitate the detection of this type of credit card fraud.

Incorrect trade capture of plain OTC derivatives transactions

The incident involved a staff member of an AI who incorrectly input the trade details of OTC derivatives transactions into the treasury system, which resulted in a material financial loss to the AI.

Modus operandi / factors leading to the incident

The AI entered into two short-maturity FX option transactions with its client. During the trade capture process, the sales staff member erroneously indicated the mode of settlement of the transactions as "deliverable", instead of "non-deliverable" as previously agreed with the client, into the AI's treasury system.

Although two incorrect trade confirmations were sent to the client, the client did confirm one transaction by mistake but did not respond to another trade confirmation. Subsequently, the AI noted the error of the trade settlement details only on the fixing date and the correct trade confirmations could only be sent to the client on the settlement date. The delay was in part also caused by public holidays and weekend, the short life of the option and inadequacies of the AI's escalation procedures (see below).

Subsequently, the AI closed out the physical currency position that was no longer required and suffered a material loss arising from the difference in exchange rates. Based on client relationship considerations, the AI absorbed the loss.

Control loopholes and lessons learnt

i. The sales staff responsible for inputting trade details should be given sufficient training on the trade capture process.

ii. As regards the incorrect trade confirmation to which the client failed to respond, the AI did not initially follow up with the client because the size of the transaction was not regarded by the responsible staff as significant. Instead of relying on the judgement of individual staff members, the AI should have set clear triggers and thresholds for follow-up action. In setting the timeframe for triggering follow-up action, regard should be made to the short-life features of some financial products.